EUROPEAN PATENT OFFICE

Patent Abstracts of Japan

PUBLICATION NUMBER : 10341212
PUBLICATION DATE : 22-12-98

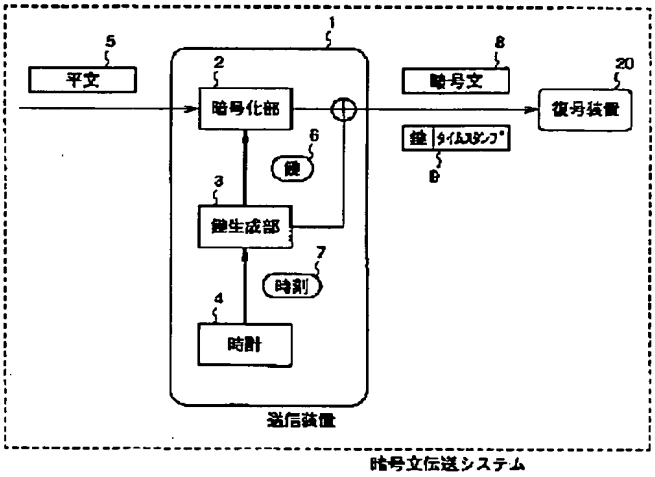
APPLICATION DATE : 10-06-97
APPLICATION NUMBER : 09152112

APPLICANT : MATSUSHITA ELECTRIC IND CO LTD;

INVENTOR : USUKI IZUMI;

INT.CL. : H04H 1/00 H04L 9/08 H04L 9/32 H04N 7/167

TITLE : ENCRYPTION TEXT TRANSMISSION SYSTEM



ABSTRACT : PROBLEM TO BE SOLVED: To allow a decoder to use discrimination information for the propriety discrimination of using an encryption key by generating the encryption key and propriety discrimination information for the use of the encryption key for decoding, generating encryption key data that relate the both and transmitting the encryption key data and encryption text data.

SOLUTION: A key generating section 3 in an encryption text transmitter 1 outputs an encryption key 6 for encryption conversion processing to an encryption processing section 2, and simultaneously the key generating section 3 obtains a current time 7 from a clock 4 and generates encryption key data relating the time 7 with the encryption key 6. On the other hand, the encryption processing section 2 uses the encryption key 6 to convert plain text data 5 into encryption text data 8, and sends the data 8, the encryption key 6, the encryption key data and an encryption key time stamp 9 to an encryption text decoder 20. In the encryption text decoder 20, when a time stamp comparator section discriminates the current time with time information of the encryption key time stamp 9 to be a key use time, encryption text data 8 are decoded. Thus, the decoder conducts decode processing by the comparison of the time for decode processing with a use time of stored data even when the data are stored.

(19)日本国特許庁（ＪＰ）　(12) **公開特許公報**（Ａ）　(11)特許出願公開番号

特開平10－341212

(43)公開日　平成10年(1998)12月22日

(51)Int.Cl.[6]		識別記号	FI		
Ｈ０４Ｈ	1/00		Ｈ０４Ｈ	1/00	Ｆ
Ｈ０４Ｌ	9/08		Ｈ０４Ｌ	9/00	６０１Ｚ
	9/32				６７１
Ｈ０４Ｎ	7/167		Ｈ０４Ｎ	7/167	Ｚ

審査請求　未請求　請求項の数９　ＯＬ　（全 11 頁）

(21)出願番号　特願平9－152112

(22)出願日　平成９年(1997)６月10日

(71)出願人　000005821
松下電器産業株式会社
大阪府門真市大字門真1006番地

(72)発明者　蒋木　泉
大阪府門真市大字門真1006番地　松下電器産業株式会社内

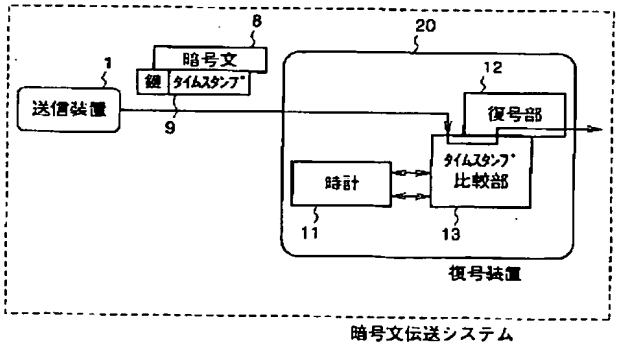
(74)代理人　弁理士　早瀬　憲一

(54)【発明の名称】　暗号文伝送システム

(57)【要約】

【課題】　暗号化されたデータを蓄積しておき、あとで復号装置に入力してデコード処理させることを防ぐ暗号文伝送システムを提供する。

【解決手段】　暗号文送信装置は、暗号化データパケット８とともに、暗号化鍵と時刻情報とからなる暗号化鍵データパケット９を送信し、暗号文復号装置２０では、パケット９から得られる時刻情報と、内蔵時計１１から得られる時刻情報とを比較することによって、復号部１２における復号処理の可否を判断する。



暗号文伝送システム

【特許請求の範囲】
【請求項１】　入力されたデータを暗号化して暗号文を送信する暗号文送信装置と、上記暗号文を復号してデータを取得する暗号文復号装置とが、伝送路を介して接続される暗号文伝送システムにおいて、
上記暗号文送信装置は、
上記入力されたデータを暗号化して、暗号文データを作成する暗号化部と、
上記暗号化に用いる暗号化鍵と、上記復号装置における上記暗号化鍵の使用の可否の判定に用いる判別情報とを作成し、
上記作成した暗号化鍵と、上記判別情報とを関連づけた暗号化鍵データを作成する鍵作成部とを備え、
上記暗号文データと上記暗号化鍵データとをともに送信することを特徴とする暗号文伝送システム。
【請求項２】　入力されたデータを暗号化して暗号文を送信する暗号文送信装置と、上記暗号文を復号してデータを取得する暗号文復号装置とが、伝送路を介して接続する暗号文伝送システムにおいて、
上記暗号文復号装置は、
送信された暗号化鍵データを復号して、暗号化鍵と、上記暗号化鍵の使用の可否の判定に用いる判別情報とを取得し、上記判別情報を後述する処理判定部に出力し、該処理判定部より許諾の信号を出力された場合に、上記暗号化鍵を用いて、送信された暗号文データを復号して平文データを取得する復号部と、
上記復号部から出力された判別情報を用いて、上記暗号化鍵の使用の可否を判定し、使用の許諾を示す信号、又は使用の拒絶を示す信号を上記復号部に出力する処理判定部とを備えたことを特徴とする暗号文伝送システム。
【請求項３】　請求項１に記載の暗号文伝送システムにおいて、
上記暗号文送信装置の上記鍵作成部は、
上記判別情報として、上記暗号化鍵の使用されるべき時刻を示す情報である使用時刻情報を作成するものであることを特徴とする暗号文伝送システム。
【請求項４】　請求項１に記載の暗号文伝送システムにおいて、
上記暗号文復号装置は、
現在時刻を示す時計を備え、
上記処理判定部は、
上記復号部から出力された使用時刻情報と、上記時計から得られる現在時刻とを比較することによって、暗号化鍵の使用されるべき時刻であるか否かを判定し、使用されるべき時刻である場合には許諾を示す信号を、使用されるべき時刻でない場合は拒絶を示す信号を上記復号部に出力する時刻情報比較部であることを特徴とする暗号文伝送システム。
【請求項５】　請求項４に記載の暗号文伝送システムにおいて、
上記暗号文復号装置は、
書き換え可能な不揮発性メモリをさらに備え、
上記時刻情報比較部は、
定期的に、上記時計から得られる現在時刻の値を上記不揮発性メモリに記録し、上記判定に際しては、上記記録した時刻と、上記時計から得られる現在時刻の値とを比較し、上記現在時刻の値が、記録した時刻の値より大きく、かつ、上記使用されるべき時刻である場合に、上記許諾を示す信号を出力するものであることを特徴とする暗号文伝送システム。
【請求項６】　請求項５に記載の暗号文伝送システムにおいて、
上記暗号文復号装置の上記時刻情報比較部は、
上記不揮発性メモリへの上記記録にあたり、上記現在時刻の値を暗号化して記録する時刻情報暗号化部を内包するものであることを特徴とする暗号文伝送システム。
【請求項７】　請求項４ないし６のいずれかに記載の暗号文伝送システムにおいて、
上記不揮発性メモリは、上記時計、上記復号部、および上記時刻情報比較部のうち一つ以上と、同一の半導体部品を構成するものであることを特徴とする暗号文伝送システム。
【請求項８】　請求項１に記載の暗号文伝送システムにおいて、
上記暗号文送信装置の上記鍵作成部は、
上記判別情報として、上記暗号文復号装置が設置されている位置を示す使用位置情報を作成するものであることを特徴とする暗号文伝送システム。
【請求項９】　請求項１に記載の暗号文伝送システムにおいて、
上記暗号文復号装置は、
当該暗号文復号装置の位置を示す、装置位置情報を獲得するためのＧＰＳ装置を備え、
上記処理判定部は、
上記復号部から出力された使用位置情報と、上記ＧＰＳ装置から得られる装置位置情報とを比較することによって、暗号化鍵の使用されるべき位置であるか否かを判定し、使用されるべき位置である場合には許諾を示す信号を、使用されるべき位置でない場合は拒絶を示す信号を上記復号部に出力する位置情報比較部であることを特徴とする暗号文伝送システム。
【発明の詳細な説明】
【０００１】
【発明の属する技術分野】本発明は、暗号文伝送システムに関し、特に入力されたデータを暗号化して暗号文を送信する暗号文送信装置と、上記暗号文を復号してデータを取得する暗号文復号装置とが、伝送路を介して接続される暗号文伝送システム、さらにはデジタル映像伝送システムでの多チャンネル映像伝送提供において、データの複製などを防止するパケットの伝送のための暗号文

伝送システムに関するものである。

【０００２】

【従来の技術】従来テレビ放送等では、アナログ信号によって送受信を行っていたが、デジタル信号を用いることによって、映像、音声、文字その他データを同等に取り扱うデジタル映像伝送システムは近年注目を集めている。

【０００３】アナログ放送が成熟段階にある現在、デジタル映像伝送システムが注目されるのは、上記のように各種データを統一的に扱い得るため、サービスの統合化を図り得る点、また、データの送受信にあたって圧縮技術を用いることにより、限定された伝送帯域幅を活用して多数の高品質な放送を行い得る点、誤り訂正技術を用いることにより均質なサービスを行い得る点、限定受信のための暗号化技術について高度な技術を容易に利用し得る点など、種々の利点があるためである。

【０００４】デジタル映像伝送システムでは、画像圧縮技術と、デジタル変復調技術とによって１中継器あたり同時に１～８番組のＴＶ番組を伝送するものであるが、画像圧縮技術については、国際規格のＭＰＥＧ２規格が採用されており、可変長符号化方式を用いて高い圧縮率を実現している。

【０００５】また、データの加工が容易であるというデジタルシステムの特性により、送信にあたって、送信データを暗号化した上で、暗文が送出されるものとすることも行われており、課金等のためや、秘密保持の確保を図るために有効な技術となっている。

【０００６】そして、データの送受信にあたっては、パケット化をすることが一般的に用いられる。パケットとは、データ全体を一定の大きさに分割したデータの単位であり、データをパケットとして送受信することによって、データ通信の効率と精度を上げることが可能となる。例えば、コンピュータネットワークにおいてパケット交換を行う場合では、それぞれのパケットはネットワークを通じて異なったタイミングで各個に転送先に届き、転送先において元のデータに再構成されるものであり、それぞれのパケットには転送先や発信元、パケットの順番などを知ることのできる情報が付加されている。

【０００７】従来の暗号文送信システムは、データの暗号化を行い、該暗号化したデータを送信する暗号文送信装置と、送信された暗号化データを復号して、元のデータを得る暗号文復号装置とから構成される。一般に暗号化は特定のビット系列である暗号化鍵を用いて、平文である通常のデータを暗号化データに変換することであり、復号は、暗号化鍵に対応する復号鍵を用いて、暗号化データを変換して平文データを取得することでなされる。ここで示すのは、特定の時間帯にのみ、暗号化したデータの復号処理をすることができ、そのデータを利用できるようにする暗号文伝送システムである。図９は、このような従来の暗号文送信装置の、また図１０は従来の暗号文復号装置の構成を示すブロック図である。

【０００８】図９において、２は暗号化部であり、平文のデータに対して暗号化鍵を用いて変換を行い、暗号化文データとする。３は鍵生成部であり、上記暗号化部の変換処理に用いる暗号化鍵を生成する。４は時計であり、現在時刻を示す。暗号化部２、鍵生成部３、および時計４は、暗号文送信装置５１を構成する。図１０において、１１は時計であり、現在時刻を示す。１２は復号部であり、暗号化されたデータを変換処理して、通常のデータを取得する。６３はタイムスタンプ比較部であり、時刻に関する情報の比較を行う。以上の時計１１、復号部１２、およびタイムスタンプ比較部６３は復号装置５２を構成する。

【０００９】以上のように構成された、従来の暗号文送信装置、及び暗号文復号装置における暗号文伝送の際の動作を説明する。まず、暗号文送信装置５１に対して、暗号化されるべき平文データ５が入力される。暗号文送信装置５１内では、鍵生成部３が暗号化の変換処理に用いる暗号化鍵を生成して、暗号化部２に出力する。それとともに鍵生成部３は、時計４から現在時刻を取得し、該現在時刻と、算出によって得る有効期限とを出力する。一方暗号化部２は、鍵生成部３が出力した暗号化鍵を用いて、平文データ５を暗号化し、暗号文を出力する。

【００１０】そして、出力された暗号化文から暗号文パケット８が、出力された鍵、鍵の有効期限、及び現在時刻から鍵パケット５９が、いずれも復号装置５２に対して伝送路を介して送信される。伝送路については、デジタル情報を伝送可能なものであればよく、例えば、衛星放送あるいは地上放送のような電波媒体、ＣＡＴＶ等有線ケーブル、またパッケージメディアであるディスク等の記録媒体のいずれでも実現される。

【００１１】伝送路より、これらのパケットが復号装置５２に入力されると、まず、復号装置５２は、時刻を示す情報の入ったパケット５９を処理し、内蔵時計１１の補正をして、内蔵時計１１を受信パケットから得られた時刻を示す情報の値に合わせてセットする。ついで、復号装置５２のタイムスタンプ比較部６３は、時計１１から得た時刻情報と、受信パケットから得られた有効期限を示す情報とを比較し、有効期限内であると判断される場合には、復号部１２に復号処理を行うように指示する。

【００１２】復号処理の指示があった場合、復号部１２は、受信パケットから得られた鍵の情報を復号鍵として用いて、暗号文パケット８から得られる暗号文データを変換処理することによって、復号データを得ることができる。一方、タイムスタンプ比較部６３による比較の際に、有効期限を過ぎたと判定された場合には、復号処理は行われず、受信データが廃棄されることとなる。

【００１３】

【発明が解決しようとする課題】上記のように、従来の暗号文送信システムでは、暗号文パケット８と、鍵、有効期限、及び時刻を示す情報からなる鍵パケット５９とを送信するものであり、復号にあたってはこの時刻を示す情報を用いて、内蔵の時計を強制的にセットすることとなる。従って、受信した暗号解読前のデータを固定ディスクなどの記憶装置に蓄積しておけば、デコード装置を持ったユーザであれば、蓄積したデータから得られる鍵、有効期限、及び時刻を示す情報を用いることにより、実際には有効期限を過ぎた場合も含み、何度でも再生することが可能となるという問題点があった。

【００１４】本発明は、かかる問題点に鑑みてなされたものであり、暗号データ送受信における時刻情報の管理によって、上記のように暗号文を蓄積しても、任意に再生することのできない暗号文伝送システムを提供することを目的とする。また、本発明は、暗号データ送受信における位置情報の管理によって、送信されたデータを受け取るべき復号装置の設置位置以外の場所での再生を防止することが可能な暗号文伝送システムを提供することを目的とする。

【００１５】

【課題を解決するための手段】上記の課題を解決するため、請求項１にかかる暗号文伝送システムは、入力されたデータを暗号化して暗号文を送信する暗号文送信装置と、上記暗号文を復号してデータを取得する暗号文復号装置とが、伝送路を介して接続される暗号文伝送システムにおいて、上記暗号文送信装置は、上記入力されたデータを暗号化して、暗号文データを作成する暗号化部と、上記暗号化に用いる暗号化鍵と、上記復号装置における上記暗号化鍵の使用の可否の判定に用いる判別情報とを作成し、上記作成した暗号化鍵と、上記判別情報とを関連づけた暗号化鍵データを作成する鍵作成部とを備え、上記暗号文データと上記暗号化鍵データとをともに送信するものである。

【００１６】また、請求項２にかかる暗号文伝送システムは、入力されたデータを暗号化して暗号文を送信する暗号文送信装置と、上記暗号文を復号してデータを取得する暗号文復号装置とが、伝送路を介して接続する暗号文伝送システムにおいて、上記暗号文復号装置は、送信された暗号化鍵データを復号して、暗号化鍵と、上記暗号化鍵の使用の可否の判定に用いる判別情報とを取得し、上記判別情報を後述する処理判定部に出力し、該処理判定部より許諾の信号を出力された場合に、上記暗号化鍵を用いて、送信された暗号文データを復号して平文データを取得する復号部と、上記復号部から出力された判別情報を用いて、上記暗号化鍵の使用の可否を判定し、使用の許諾を示す信号、又は使用の拒絶を示す信号を上記復号部に出力する処理判定部とを備えたものである。

【００１７】また、請求項３にかかる暗号文伝送システムは、請求項１に記載の暗号文伝送システムにおいて、上記暗号文送信装置の上記鍵作成部は、上記判別情報として、上記暗号化鍵の使用されるべき時刻を示す情報である使用時刻情報を作成するものである。

【００１８】また、請求項４にかかる暗号文伝送システムは、請求項１に記載の暗号文伝送システムにおいて、上記暗号文復号装置は、現在時刻を示す時計を備え、上記処理判定部は、上記復号部から出力された使用時刻情報と、上記時計から得られる現在時刻とを比較することによって、暗号化鍵の使用されるべき時刻であるか否かを判定し、使用されるべき時刻である場合には許諾を示す信号を、使用されるべき時刻でない場合は拒絶を示す信号を上記復号部に出力する時刻情報比較部であるものである。

【００１９】また、請求項５にかかる暗号文伝送システムは、請求項４に記載の暗号文伝送システムにおいて、上記暗号文復号装置は、書き換え可能な不揮発性メモリをさらに備え、上記時刻情報比較部は、定期的に、上記時計から得られる現在時刻の値を上記不揮発性メモリに記録し、上記判定に際しては、上記記録した時刻と、上記時計から得られる現在時刻の値とを比較し、上記現在時刻の値が、記録した時刻の値より大きく、かつ、上記使用されるべき時刻である場合に、上記許諾を示す信号を出力するものである。

【００２０】また、請求項６にかかる暗号文伝送システムは、請求項５に記載の暗号文伝送システムにおいて、上記暗号文復号装置の上記時刻情報比較部は、上記不揮発性メモリへの上記記録にあたり、上記現在時刻の値を暗号化して記録する時刻情報暗号化部を内包するものである。

【００２１】また、請求項７にかかる暗号文伝送システムは、請求項４ないし６のいずれかに記載の暗号文伝送システムにおいて、上記不揮発性メモリは、上記時計、上記復号部、および上記時刻情報比較部のうち一つ以上と、同一の半導体部品を構成するものである。

【００２２】また、請求項８にかかる暗号文伝送システムは、請求項１に記載の暗号文伝送システムにおいて、上記暗号文送信装置の上記鍵作成部は、上記判別情報として、上記暗号文復号装置が設置されている位置を示す使用位置情報を作成するものである。

【００２３】また、請求項９にかかる暗号文伝送システムは、請求項１に記載の暗号文伝送システムにおいて、上記暗号文復号装置は、当該暗号文復号装置の位置を示す、装置位置情報を獲得するためのＧＰＳ装置を備え、上記処理判定部は、上記復号部から出力された使用位置情報と、上記ＧＰＳ装置から得られる装置位置情報とを比較することによって、暗号化鍵の使用されるべき位置であるか否かを判定し、使用されるべき位置である場合には許諾を示す信号を、使用されるべき位置でない場合は拒絶を示す信号を上記復号部に出力する位置情報比較

部であるものである。

【００２４】

【発明の実施の形態】

実施の形態１．本発明の実施の形態１による暗号文伝送システムは、暗号化鍵と、その鍵を用いることができる使用時刻情報とを関連づけて伝送するものである。図１は、本発明の実施の形態１による暗号文送信装置の構成を、又、図２は、本実施の形態１による暗号文復号装置の構成を示すブロック図である。図１において、２は暗号化部であり、平文のデータに対して、後述する鍵生成部３が作成する暗号化鍵を用いて変換を行い、暗号化文データを作成する。３は鍵生成部であり、上記暗号化部の変換処理に用いる暗号化鍵を作成するとともに、該生成した暗号化鍵と、現在時刻に基づく使用時刻情報とを関連づけた暗号化鍵データを作成する。４は時計であり、現在時刻を示す。以上の暗号化部２、鍵生成部３、および時計４は、暗号文送信装置１を構成する。また、図２において、１１は時計であり、現在時刻を示す。１２は復号部であり、暗号化鍵に対応する復号鍵を用いて、暗号化されたデータを変換処理し、通常のデータである平文データを取得する。１３はタイムスタンプ比較部であり、時刻に関する情報の比較を行う。以上の時計１１、復号部１２、およびタイムスタンプ比較部１３は復号装置２０を構成する。

【００２５】以上のように構成された、本実施の形態１の暗号文送信装置、及び暗号文復号装置における暗号文伝送の際の動作を説明する。まず、暗号文送信装置１に対して、暗号化されるべき平文データ５が入力される。暗号文送信装置１内では、鍵生成部３が、所定の方式に従って生成するビット系列を、暗号化の変換処理に用いる暗号化鍵として暗号化部２に出力する。それとともに鍵生成部３は、時計４から現在時刻７を取得し、該現在時刻７と、上記の暗号化鍵とを関連づけた暗号化鍵データを作成する。一方暗号化部２は、鍵生成部３が出力した暗号化鍵６を用いて、平文データ５を変換処理することによって暗号化し、暗号文データを出力する。

【００２６】そして、出力された暗号文データから暗号文パケット８が、出力された暗号化鍵データから暗号化鍵パケット９が、いずれも復号装置２０に対して、従来例と同様に伝送路を介して送信される。

【００２７】伝送路より、これらのパケットが復号装置２０に入力されると、まず、復号装置２０の復号部１２は、暗号化鍵パケット９を処理することにより、使用時刻情報を取得し、これをタイムスタンプ比較部１３に出力する。タイムスタンプ比較部１３は、時計１１から現在時刻情報を取得し、この現在時刻情報と、上記のように復号部１２から出力された使用時刻情報とを比較し、使用時刻情報に基づく所定の範囲内に、現在時刻情報が該当する場合は「鍵が使用されるべき時刻である」という判断をし、該当しない場合は、「鍵が使用されるべき時刻でない」という判断をする。そして鍵が使用されるべき時刻であると判断する場合は、許諾の信号を、そうでない場合は拒絶の信号を復号部１２に出力する。

【００２８】復号部１２は、許諾の信号を出力された場合は、暗号化鍵パケットから得られた鍵の情報を復号鍵として用いて、暗号文パケット８から得られる暗号文データを変換処理することによって、復号データを得る。一方、拒絶の信号を出力された場合には、復号処理は行われず、受信データが廃棄されることとなる。

【００２９】このように、本実施の形態１による暗号文伝送システムは、暗号化部２、鍵作成部３、及び時計４とを備えた暗号文送信装置１と、内蔵時計１１、復号部１２、及びタイムスタンプ比較部１３を備えた暗号文復号装置２０とから構成されるものとしたことで、暗号文送信装置１において作成した暗号化鍵と、該作成した時刻とを関連づけた暗号化鍵データを、暗号化鍵パケット９として送信し、これを受信した復号装置２０では、内蔵時計１１から得られる現在時刻と、暗号化鍵パケット９から得られる時刻の情報とを比較することによって、タイムスタンプ比較部１３が、鍵が使用されるべき時刻であるか否かを判定し、使用されるべき時刻である場合にのみ、暗号文パケット８の暗号文データが復号処理されることとなる。従って、従来例に示した暗号文伝送システムのように、復号装置２０の時計１１がリセットされることがなく、かりにデータを蓄積した場合にも、復号処理を行おうとする際の時刻と、該蓄積したデータより取得する使用時刻情報との比較により、復号処理は行われないこととなる。

【００３０】実施の形態２．本発明の実施の形態２による暗号文伝送システムは、実施の形態１と同様に使用時刻情報が用いられるものであり、復号装置は現在時刻を使用時刻情報と比較するにあたり、現在時刻の確認処理を行うものである。

【００３１】図３は、本実施の形態２による暗号文伝送システムの構成を示すブロック図である。図において、暗号文送信装置１は、実施の形態１と同じものであり、同様に暗号文パケット８と、暗号化鍵パケット９とを送信する。暗号文復号装置２１の１４は不揮発性メモリであり、電源切断時にも記憶内容を保持し得るメモリである。他は図２と同じであり、説明は実施の形態１と同じである。

【００３２】このように構成される、本実施の形態２による暗号文伝送システムの復号装置２１による復号処理の動作を以下に説明する。本実施の形態２の復号装置２１は、設定された周期（Tw時間）ごとに内蔵時計１１の値を不揮発性メモリ１４に書き込みを行うものである。書き込まれた時刻を示す情報は、記憶時刻情報として保持される。

【００３３】ここで、実施の形態１と同様に、暗号文パケット８と、暗号化鍵パケット９とが復号装置２１に入

力されたとする。復号部１２は、暗号化鍵パケット９を処理することにより、使用時刻情報を取得し、これをタイムスタンプ比較部１３に出力する。

【００３４】タイムスタンプ比較部１３による判定処理は実施の形態１と異なり、以下のように行われる。まず、第１の比較処理として、タイムスタンプ比較部１３は、不揮発性メモリ１４から記憶時刻情報を読み出し、時計１１から取得した現在時刻情報との比較を行う。そして、記憶時刻情報が現在時刻情報の値以下の場合は、記憶時刻情報の値を内蔵時計１１の値に書き換え、不正は無いと判断する。一方、記憶時刻情報の値が、現在時刻情報の値より大きい場合は、内蔵時計１１の示す時刻に不正があると判断し、後述する第２の比較処理を行うことなく、復号部１２に対して拒絶の信号を出力することにより、復号動作を禁止する。

【００３５】第１の比較処理において、内蔵時計１１の不正が検出されない場合、第２の比較処理が行われ、実施の形態１と同様に、使用時刻情報と現在時刻情報とが比較される。第２の比較の結果、復号又は廃棄処理が行われる点は、実施の形態１と同様である。

【００３６】従って、タイムスタンプ比較部１３による比較処理では、第１の比較処理において、内蔵時計１１の不正がなく、かつ、実施の形態１と同様に、使用可能な時刻であると判定される場合にのみ、許諾の信号が出力されるものであり、復号部１２での暗号文の復号が行われる。

【００３７】このように、本実施の形態２による暗号文伝送システムでは、復号装置２１が不揮発性メモリ１４をさらに備えたことで、定期的に内蔵する時計１１の示す時刻を該不揮発性メモリ１４に書き込み、復号化の前には、書き込んだ記憶時刻情報と、内蔵の時計の示す現在時刻情報とを比較することで、時計１１の改竄を検出する。従って、従来の技術による暗号文送信システムや、実施の形態１のシステムではすることのできない、時計１１の改竄による不正デコード動作の防止をすることが可能となる。

【００３８】実施の形態３．本発明の実施の形態３による暗号文伝送システムは、実施の形態２と同様、復号装置が、現在時刻の確認処理を行うものである。図４は、本実施の形態３による暗号文伝送システムの構成を示すブロック図である。図において、暗号文送信装置１は、実施の形態１と同じものであり、同様に暗号文パケット８と、暗号化鍵パケット９とを送信する。暗号文復号装置２１'では、不揮発性メモリ１４と時計１１とが、同一チップ１６上にあること以外は、実施の形態２と同じである。そして、本実施の形態３の復号装置２１'の動作も又、実施の形態２と同じである。

【００３９】このように、本実施の形態３による暗号文伝送システムでは、不揮発性メモリ１４と内蔵時計１１を同一のチップ１６内におくものとする構成によって、外部からの不揮発性メモリ１４内に記憶された情報の書き換えをなすことを防止し、実施の形態２よりも有効な不正の防止が可能となる。

【００４０】実施の形態４．本発明の実施の形態４による暗号文伝送システムは、実施の形態２と同様、復号装置が、現在時刻の確認処理を行うものである。図５は、本実施の形態４による暗号文伝送システムの構成を示すブロック図である。図において、暗号文送信装置１は、実施の形態１と同じものであり、同様に暗号文パケット８と、暗号化鍵パケット９とを送信する。暗号文復号装置２２の１５は時刻暗号化部であり、内蔵の時計１１から取得する現在の時刻を暗号化した上で、暗号化記憶時刻情報として不揮発性メモリ１４に書き込む。他は図３と同じであり、説明は実施の形態２と同じである。また、本実施の形態４の復号装置２２の動作は、不揮発性メモリ１４に書き込まれる時刻情報が暗号化されたものである点を除いては、実施の形態２と同じである。

【００４１】このように、本実施の形態４による暗号文伝送システムでは、復号装置２２が時刻暗号化部１５を備えたものとしたことで、不揮発性メモリ１４に不揮発性メモリ１４内に記憶された情報を暗号化されたものとすることで、外部からの書き換えをなすことを防止し、実施の形態３と同様に、有効な不正の防止が可能となる。

【００４２】実施の形態５．本発明の実施の形態５による暗号文伝送システムは、暗号化鍵と、その鍵を用いることができる使用位置情報とを関連づけて伝送するものである。図６は、本発明の実施の形態５による暗号文送信装置の構成を、又、図７は、本実施の形態５による暗号文復号装置の構成を示すブロック図である。本実施の形態５の暗号文伝送システムは、暗号文送信装置３１と、暗号文復号装置２４とから構成される。図６において、１０は受信位置データベースであり、暗号化されたデータを受信すべき復号装置の設置位置についての情報を記憶するデータベースである。図７において、１１'は内蔵ＧＰＳであり、ＧＰＳ衛星からの電波信号による情報に基づいて、現在の緯度と経度を算出する。１３'は位置情報比較部であり、位置に関する情報の比較を行う。他は図１～２と同じであり、説明は実施の形態１と同じである。

【００４３】以上のように構成された、本実施の形態５の暗号文送信装置、及び暗号文復号装置における暗号文伝送の際の動作を説明する。まず、暗号文送信装置３１に対して、暗号化されるべき平文データ５が入力される。暗号文送信装置１内では、鍵生成部３が、あるビット系列を生成し、これを暗号化の変換処理に用いる暗号化鍵として暗号化部２に出力する。それとともに鍵生成部３は、受信位置データベース１０から送信すべき相手である受信装置の設置位置に関する使用位置情報７'を取得し、使用位置情報７'と、上記の暗号化鍵とを関連

づけた暗号化鍵データを作成する。一方暗号化部２は、鍵生成部３が出力した暗号化鍵を用いて、平文データ５を変換処理することによって暗号化し、暗号文データを出力する。

【００４４】そして、出力された暗号文データから暗号文パケット８が、出力された暗号化鍵データから暗号化鍵パケット９'が、いずれも復号装置２４に対して、従来例と同様に伝送路を介して送信される。

【００４５】伝送路より、これらのパケットが復号装置２４に入力されると、まず、復号装置２４の復号部１２は、暗号化鍵パケット９'を処理することにより、使用位置情報を取得し、これを位置情報比較部１３'に出力する。位置情報比較部１３'は、内蔵ＧＰＳ１１'から現在位置情報を取得し、この現在位置情報と、上記のように復号部１２から出力された使用位置情報とを比較し、使用位置情報に基づく所定の範囲内に、現在位置情報が該当する場合は「鍵が使用されるべき位置である」という判断をし、該当しない場合は、「鍵が使用されるべき位置でない」という判断をする。そして鍵が使用されるべき位置であると判断する場合は、許諾の信号を、そうでない場合は拒絶の信号を復号部１２に出力する。

【００４６】復号部１２は、許諾の信号を出力された場合は、暗号化鍵パケットから得られた鍵の情報を復号鍵として用いて、暗号文パケット８から得られる暗号文データを変換処理することによって、復号データを得る。一方、拒絶の信号を出力された場合には、復号処理は行われず、受信データが廃棄されることとなる。

【００４７】このように、本実施の形態５による暗号文伝送システムは、暗号化部２、鍵作成部３、及び受信位置データベース１０を備えた暗号文送信装置３１と、内蔵ＧＰＳ１１'、復号部１２、及び位置情報比較部１３'を備えた暗号文復号装置２４とから構成されるものとしたことで、暗号文送信装置３１において作成した暗号化鍵と、受信されるべき位置とを関連づけた暗号化鍵データを、暗号化鍵パケット９'として送信し、これを受信した復号装置２４では、内蔵ＧＰＳ１１'から得られる現在位置と、暗号化鍵パケット９'から得られる使用すべき位置の情報とを比較することによって、位置情報比較部１３'が、鍵が使用されるべき位置であるか否かを判定し、使用されるべき位置である場合にのみ、暗号文パケット８の暗号文データが復号処理されることとなる。従って、全データを蓄積して別の場所で受信装置に入力しても復号できなくすることができるので、不正な傍受を防ぐことができる。

【００４８】実施の形態６．本発明の実施の形態６による暗号文伝送システムは、復号装置がバスを有する構成としたものである。図８は、本実施の形態６による暗号文伝送システムの構成を示すブロック図である。図において、暗号文送信装置１は、実施の形態１と同じものであり、同様のパケットを送信する。復号装置２３の１７はバスであり、装置の各部分が信号をやりとりするための、共通の信号路である。１８はＩＦ（インタフェイス）であり、装置の外部とのデータの授受を制御する。１９はＣＰＵであり、数値演算や装置各部の機能の制御を行う。１１～１３は実施の形態２と、１４は実施の形態３と、１５は実施の形態４と同様である。

【００４９】このように構成される本実施の形態６による復号装置２３では、送信装置１から伝送されたデータがＩＦ１８を通して入力され、１１～１５が、ＣＰＵ１９の制御のもとに、バス１７によってデータのやりとりを行うことにより、実施の形態１～４の復号装置と同様に動作することとなる。

【００５０】本実施の形態６による暗号文伝送システムでは、復号装置２３が、バス１７、ＩＦ１８、及びＣＰＵ１９を備えたものとしたことで、汎用的な構成により、暗号化されたデータの復号処理をすることを可能とする。

【００５１】なお、本実施の形態６では、時計１１とタイムスタンプ比較部１３とを備えたものとしたことで、実施の形態１～４の復号装置を実現するものであるが、内蔵ＧＰＳと、位置情報比較部とを備えたものとすることで、実施の形態５の復号装置を実現することも可能である。

【００５２】

【発明の効果】請求項１の暗号文伝送システムによれば、入力されたデータを暗号化して暗号文を送信する暗号文送信装置と、上記暗号文を復号してデータを取得する暗号文復号装置とが、伝送路を介して接続する暗号文伝送システムにおいて、上記暗号文送信装置は、上記入力されたデータを暗号化して、暗号文データを作成する暗号化部と、上記暗号化に用いる暗号化鍵と、上記復号装置における上記暗号化鍵の使用の可否の判定に用いる判別情報とを作成し、上記作成した暗号化鍵と、上記判別情報とを関連づけた暗号化鍵データを作成する鍵作成部とを備え、上記暗号文データと上記暗号化鍵データとをともに送信するものとしたことで、復号装置が暗号化鍵の使用の可否の判定に判別情報を用いることを可能とする。

【００５３】また、請求項２の暗号文伝送システムによれば、入力されたデータを暗号化して暗号文を送信する暗号文送信装置と、上記暗号文を復号してデータを取得する暗号文復号装置とが、伝送路を介して接続する暗号文伝送システムにおいて、上記暗号文復号装置は、送信された暗号化鍵データを復号して、暗号化鍵と、上記暗号化鍵の使用の可否の判定に用いる判別情報とを取得し、上記判別情報を後述する処理判定部に出力し、該処理判定部より許諾の信号を出力された場合に、上記暗号化鍵を用いて、送信された暗号文データを復号して平文データを取得する復号部と、上記復号部から出力された判別情報を用いて、上記暗号化鍵の使用の可否を判定

し、使用の許諾を示す信号、又は使用の拒絶を示す信号を上記復号部に出力する処理判定部とを備えたものとしたことで、判別情報を用いた判定を行うことにより、不正な復号処理を防止することが可能となる。

【００５４】また、請求項３の暗号文伝送システムによれば、請求項１に記載の暗号文伝送システムにおいて、上記暗号文送信装置の上記鍵作成部は、上記判別情報として、上記暗号化鍵の使用されるべき時刻を示す情報である使用時刻情報を作成するものとしたことで、判別情報として時刻を用いることを可能とする。

【００５５】また、請求項４の暗号文伝送システムによれば、請求項１に記載の暗号文伝送システムにおいて、上記暗号文復号装置は、現在時刻を示す時計を備え、上記処理判定部は、上記復号部から出力された使用時刻情報と、上記時計から得られる現在時刻とを比較することによって、暗号化鍵の使用されるべき時刻であるか否かを判定し、使用されるべき時刻である場合には許諾を示す信号を、使用されるべき時刻でない場合は拒絶を示す信号を上記復号部に出力する時刻情報比較部であるものとしたことで、鍵が用いられるべき期間以外における復号化処理を防止することが可能となる。

【００５６】また、請求項５の暗号文伝送システムによれば、請求項４に記載の暗号文伝送システムにおいて、上記暗号文復号装置は、書き換え可能な不揮発性メモリをさらに備え、上記時刻情報比較部は、定期的に、上記時計から得られる現在時刻の値を上記不揮発性メモリに記録し、上記判定に際しては、上記記録した時刻と、上記時計から得られる現在時刻の値とを比較し、上記現在時刻の値が、記録した時刻の値より大きく、かつ、上記使用されるべき時刻である場合に、上記許諾を示す信号を出力するものとしたことで、内蔵時計の改竄を検出することができ、蓄積データを用いての不正な復号処理を防止することが可能となる。

【００５７】また、請求項６の暗号文伝送システムによれば、請求項５に記載の暗号文伝送システムにおいて、上記暗号文復号装置の上記時刻情報比較部は、上記不揮発性メモリへの上記記録にあたり、上記現在時刻の値を暗号化して記録する時刻情報暗号化部を内包するものとしたことで、内蔵時計の改竄を検出でき、該検出にあたっての不揮発性メモリに記録された内容の改竄をも防止し得るので、蓄積データを用いての不正な復号処理の防止の実効を図れる。

【００５８】また、請求項７の暗号文伝送システムによれば、請求項４ないし６のいずれかに記載の暗号文伝送システムにおいて、上記不揮発性メモリは、上記時計、上記復号部、および上記時刻情報比較部のうち一つ以上と、同一の半導体部品を構成するものとしたことで、外部から直接不揮発性メモリにアクセスすることを防止することによって、不揮発性メモリ内のデータの改竄を防ぎ、蓄積データを用いての不正な復号処理の防止の実効を図れる。

【００５９】また、請求項８の暗号文伝送システムによれば、請求項１に記載の暗号文伝送システムにおいて、上記暗号文送信装置の上記鍵作成部は、上記判別情報として、上記暗号文復号装置が設置されている位置を示す使用位置情報を作成するものとしたことで、判別情報として位置を示す情報を用いることを可能とする。

【００６０】また、請求項９の暗号文伝送システムによれば、請求項１に記載の暗号文伝送システムにおいて、上記暗号文復号装置は、当該暗号文復号装置の位置を示す、装置位置情報を獲得するためのＧＰＳ装置を備え、上記処理判定部は、上記復号部から出力された使用位置情報と、上記ＧＰＳ装置から得られる装置位置情報とを比較することによって、暗号化鍵の使用されるべき位置であるか否かを判定し、使用されるべき位置である場合には許諾を示す信号を、使用されるべき位置でない場合は拒絶を示す信号を上記復号部に出力する位置情報比較部であるものとしたことで、鍵が用いられるべき地域以外における復号化処理を防止することが可能となる。

【図面の簡単な説明】

【図１】本発明の実施の形態１による暗号文送信装置の構成を示すブロック図である。

【図２】本発明の実施の形態１による暗号文復号装置の構成を示すブロック図である。

【図３】本発明の実施の形態２による暗号文復号装置の構成を示すブロック図である。

【図４】本発明の実施の形態３による暗号文復号装置の構成を示すブロック図である。

【図５】本発明の実施の形態４による暗号文復号装置の構成を示すブロック図である。

【図６】本発明の実施の形態５による暗号文送信装置の構成を示すブロック図である。

【図７】本発明の実施の形態５による暗号文復号装置の構成を示すブロック図である。

【図８】本発明の実施の形態６による暗号文復号装置の構成を示すブロック図である。

【図９】従来の技術による暗号文送信装置の構成を示すブロック図である。

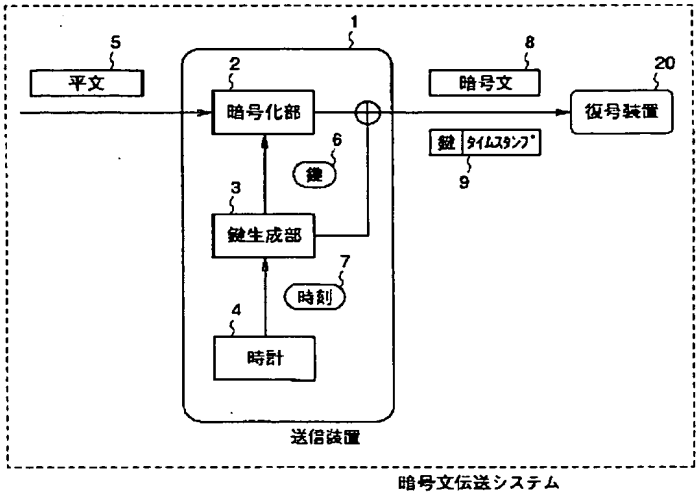
【図１０】従来の技術による暗号文送信装置の構成を示すブロック図である。

【符号の説明】

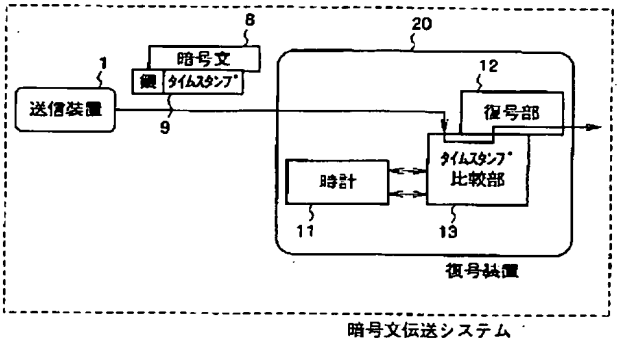
１，３１，５１　暗号文送信装置
２　暗号化部
３　鍵生成部
４　時計
５　平文
６　鍵
７　時刻情報
７'　位置情報
８　暗号文データパケット

9，9'　暗号化鍵データパケット
59　暗号化鍵パケット
20，21，21'，22，23，24，52　暗号文復号装置
11　内蔵時計
11'　内蔵GPS
12　復号部
13，63　タイムスタンプ比較部
14　不揮発性メモリ
15　時刻暗号化部
16　時計及び不揮発性メモリ内蔵チップ
17　バス
18　インタフェース
19　CPU

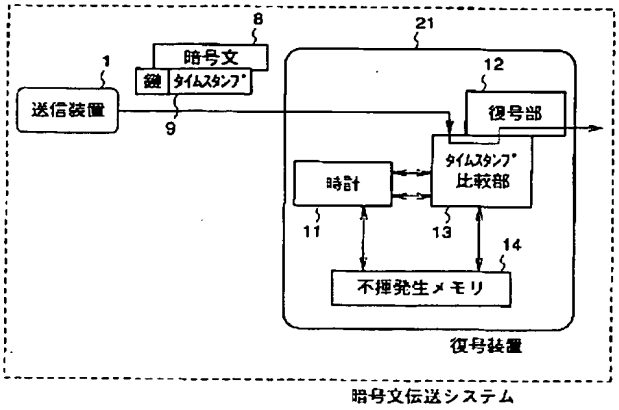
【図1】



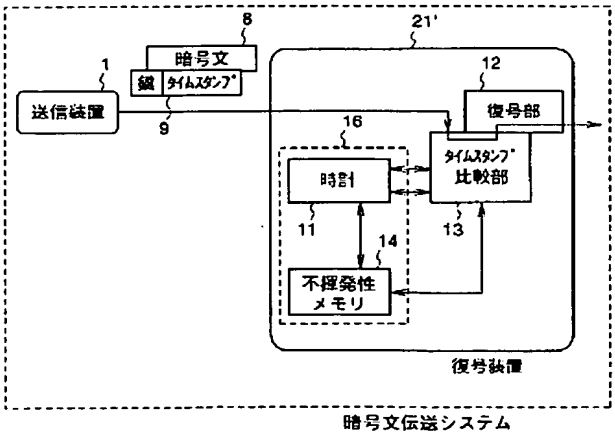
【図2】



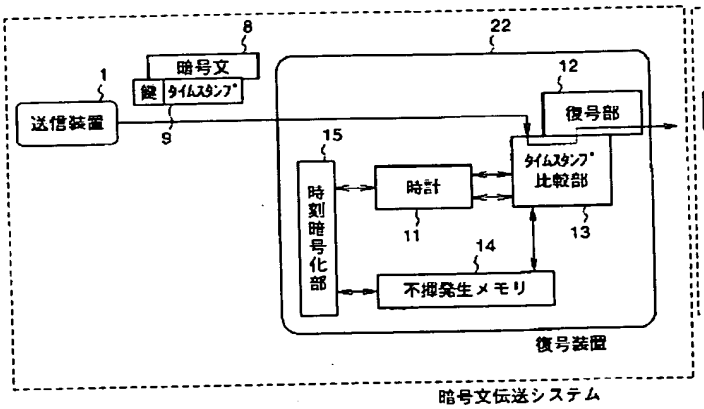
【図3】



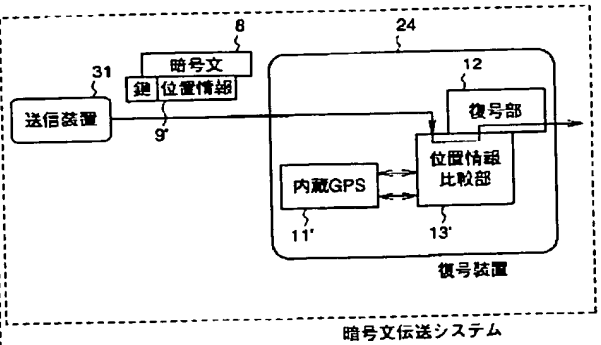
【図4】



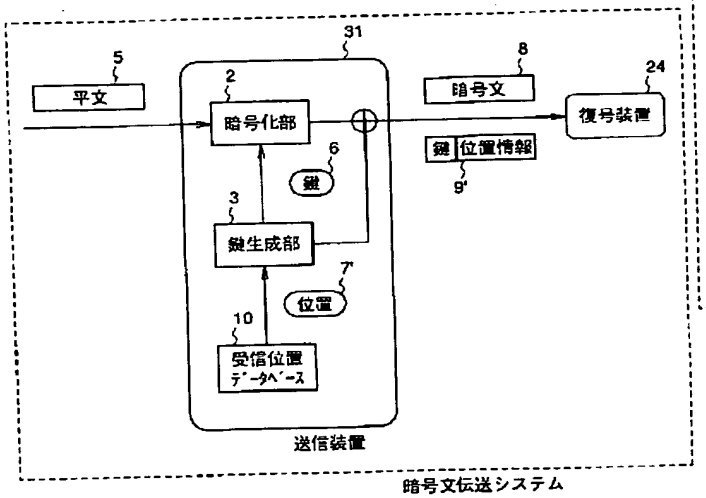
【図5】



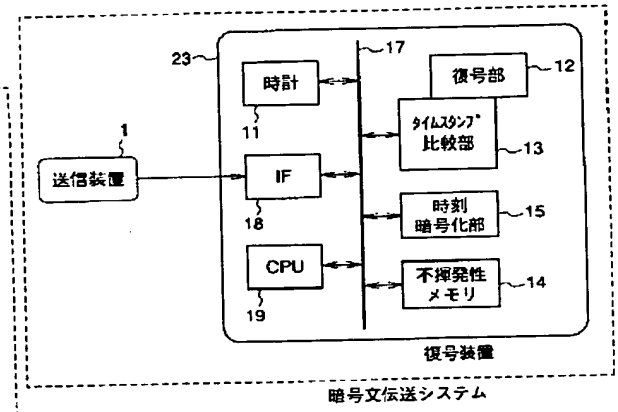
【図7】



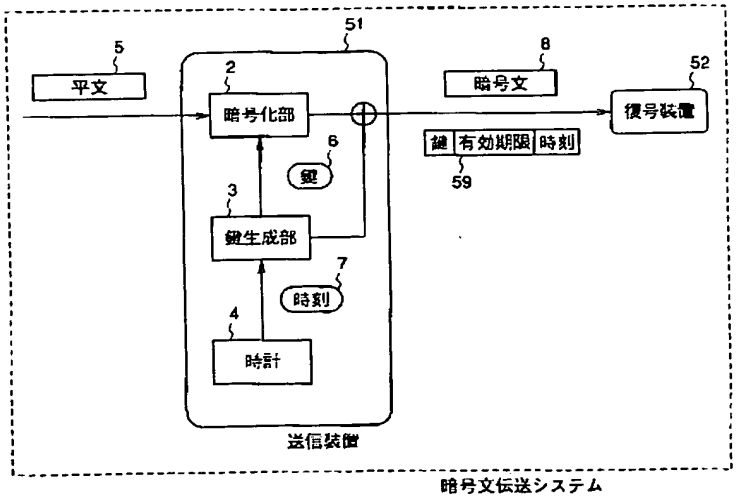
【図6】



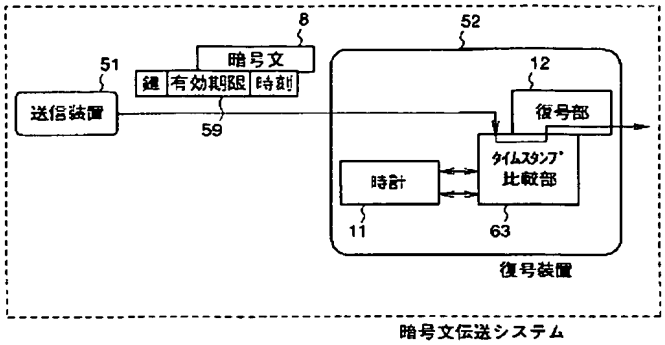
【図8】



【図9】



【図10】



This page blank (usptо)